修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　電気通信　学研究科　情報通信工学　専攻　博士前期課程		
氏　　名	宮川　聡	学籍番号	0630063
論 文 題 目	Relation among Notions for Public-Key Encryption Scheme		

要　旨

公開鍵暗号方式の証明可能安全性は，セキュリティゴールと攻撃シナリオの 2 つの要素の組み合わせで定義される．セキュリティゴールとは，公開鍵暗号方式における攻撃者が達成したい解読レベルを定式化したものであり，攻撃シナリオとは，攻撃者に許された行動をモデル化したものである．セキュリティゴールの中で最も達成が困難な概念が頑健性（NM）である．公開鍵暗号方式にとって，この頑健性を攻撃シナリオが攻撃者の行動が最大限に許されている適応的選択暗号文攻撃(CCA2)のときでも満たすことが最終目的となる．

公開鍵暗号方式の証明可能安全性を示す際に用いられるモデルの中にランダムオラクルモデル（ROM）がある．ROM とは，ランダムオラクルと呼ばれるプロトコルを実行する全てのパーティ及び攻撃者が利用可能なランダム関数のことで，ハッシュ関数を理想化した状態で証明可能安全性を示す手法である．ROM では，ランダムオラクルを実際のハッシュ関数に置き換えると安全性が崩れてしまう公開鍵暗号方式, 署名方式が存在することが知られている．しかし, ROM は，未だ暗号プロトコルを構成する際の指針として重要な役割を持っている．

公開鍵暗号方式にとって重要な NM と ROM にはそれぞれ，NM では定義において定義中と証明中で暗号文に関する制限の扱いが整合していない問題，ROM には，方式によってランダムオラクルへの依存度が異なるにも関わらず，全てが同一の ROM として証明可能安全性が示されている問題がある．

本研究では，NM に関しては，定義中と証明中で制限の扱いが整合していない問題に関して差が存在するか否かを明らかにし，ROM に関しては，新しい ROM として，攻撃者にハッシュリストの閲覧の能力を与えた ROM を提案する．またこのモデルを用いて，暗号プロトコル（OAEP, Fujisaki-Okamoto 変換，PFDH）におけるランダムオラクルへの依存度についても考察する．